



Out-Of-Band Meraki

UCOPIA Communications

Cloud Meraki

- 84.14.161.21
- 84.14.161.29
- 185.17.255.128/25
- 185.92.120.0/25
- 50.115.86.96/27
- 217.89.128.0/24

(cf. **dashboard « Help > Firewall information »**)



Firewall

10.0.0.1

→ Correct FW openings rules need to be applied so that Meraki AP can communicate with Cloud Meraki



Central UCOPIA

172.16.10.150

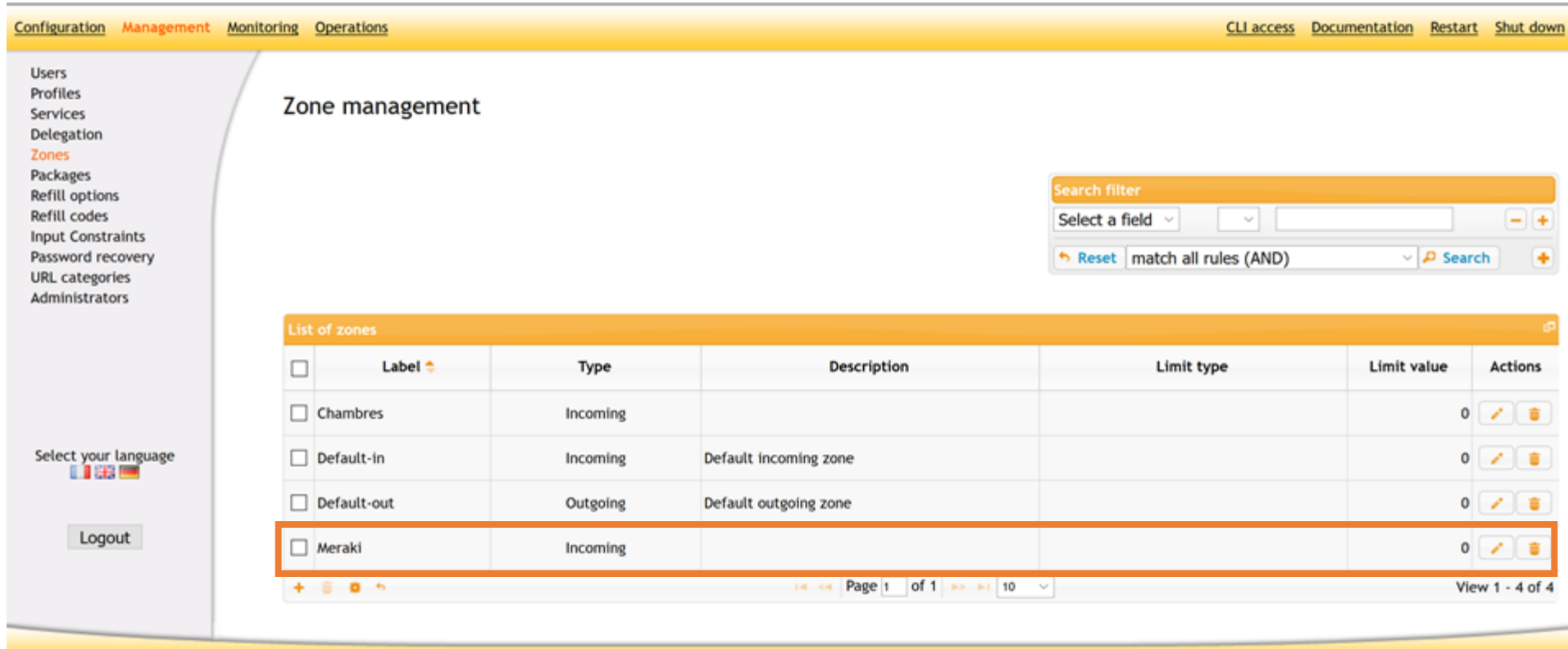
cloud1.ucopia.com



Meraki AP

10.0.1.111 (DHCP)









Create the concerned zone (e.g. « Meraki »)



The screenshot shows the UCOPIA web interface for zone management. The top navigation bar includes links for Configuration, Management, Monitoring, and Operations. A sidebar on the left lists various configuration options, with 'Zones' highlighted. The main content area is titled 'Zone management' and features a search filter box and a table of zones. The 'Meraki' zone is highlighted in the table.

Zone management

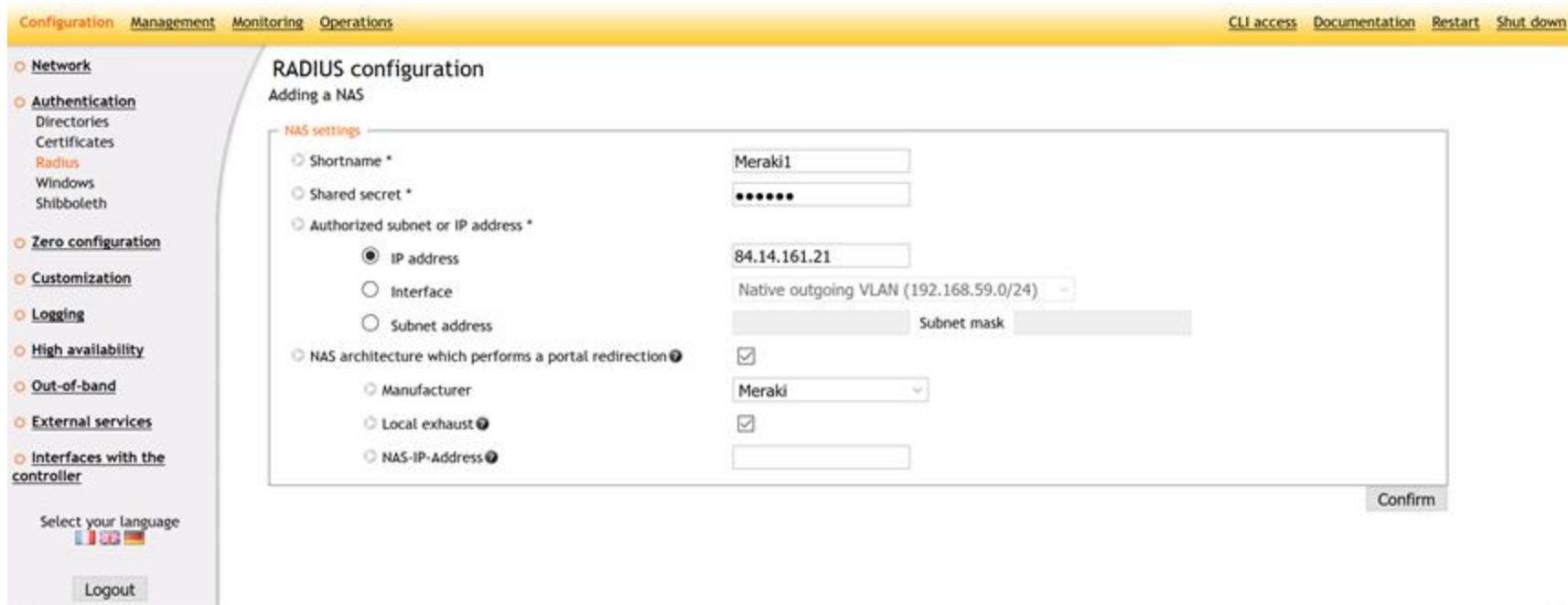
Search filter: Select a field, Reset, match all rules (AND), Search

	Label	Type	Description	Limit type	Limit value	Actions
<input type="checkbox"/>	Chambres	Incoming			0	 
<input type="checkbox"/>	Default-in	Incoming	Default incoming zone		0	 
<input type="checkbox"/>	Default-out	Outgoing	Default outgoing zone		0	 
<input type="checkbox"/>	Meraki	Incoming			0	 

Page 1 of 1, View 1 - 4 of 4

Create as many NAS configuration in the central UCOPIA as needed for the inbound traffic:

- 84.14.161.21
- 84.14.161.29
- 185.17.255.128/25
- 185.92.120.0/25
- 50.115.86.96/27
- 217.89.128.0/24



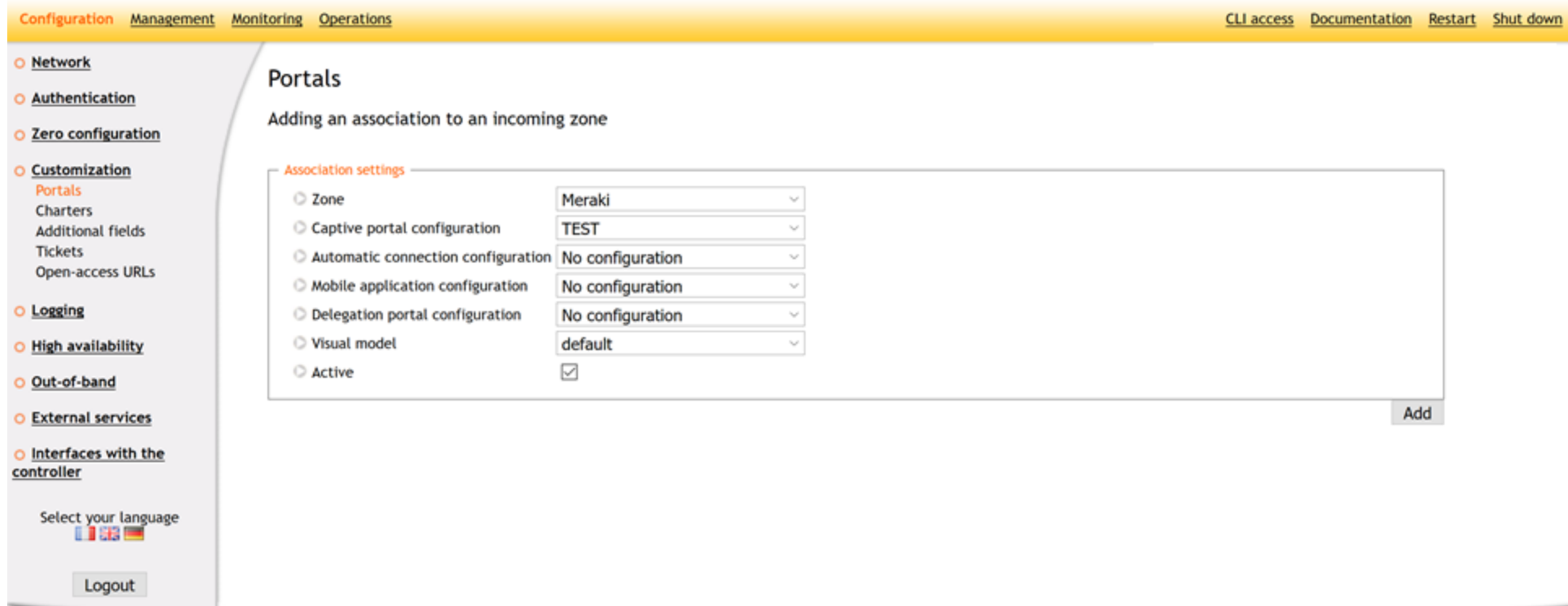
The screenshot displays the UCOPIA web interface. The top navigation bar includes links for Configuration, Management, Monitoring, and Operations, along with utility links for CLI access, Documentation, Restart, and Shut down. A left sidebar contains a tree view of configuration categories: Network, Authentication (with sub-items Directories, Certificates, Radius, Windows, and Shibboleth), Zero configuration, Customization, Logging, High availability, Out-of-band, External services, and Interfaces with the controller. At the bottom of the sidebar are language selection options and a Logout button.

The main content area is titled "RADIUS configuration" and "Adding a NAS". It features a "NAS settings" section with the following fields and options:

- Shortname ***: Text input field containing "Meraki1".
- Shared secret ***: Password input field with masked characters.
- Authorized subnet or IP address ***:
 - ☒ **IP address**: Text input field containing "84.14.161.21".
 - ☐ **Interface**: Dropdown menu showing "Native outgoing VLAN (192.168.59.0/24)".
 - ☐ **Subnet address**: Two adjacent text input fields for Subnet and mask.
- ☒ **NAS architecture which performs a portal redirection**:
 - ☐ **Manufacturer**: Dropdown menu showing "Meraki".
 - ☒ **Local exhaust**: Checkmark.
 - ☐ **NAS-IP-Address**: Text input field.

A "Confirm" button is located at the bottom right of the configuration form.

Create a portal association on the concerned zone (e.g. « Meraki »):



The screenshot displays the UCOPIA configuration web interface. At the top, a yellow navigation bar contains links for Configuration, Management, Monitoring, and Operations. On the right side of this bar are links for CLI access, Documentation, Restart, and Shut down. A left-hand sidebar lists various configuration categories: Network, Authentication, Zero configuration, Customization (with sub-items: Portals, Charters, Additional fields, Tickets, Open-access URLs), Logging, High availability, Out-of-band, External services, and Interfaces with the controller. Below these is a language selection option and a Logout button. The main content area is titled 'Portals' and includes the subtitle 'Adding an association to an incoming zone'. It features a form titled 'Association settings' with the following fields: Zone (set to 'Meraki'), Captive portal configuration (set to 'TEST'), Automatic connection configuration (set to 'No configuration'), Mobile application configuration (set to 'No configuration'), Delegation portal configuration (set to 'No configuration'), Visual model (set to 'default'), and Active (checked). An 'Add' button is located at the bottom right of the form.

Configuration Management Monitoring Operations CLI access Documentation Restart Shut down

Network
Authentication
Zero configuration
Customization
Portals
Charters
Additional fields
Tickets
Open-access URLs
Logging
High availability
Out-of-band
External services
Interfaces with the controller

Select your language
Logout

Portals

Adding an association to an incoming zone

Association settings

Zone	Meraki
Captive portal configuration	TEST
Automatic connection configuration	No configuration
Mobile application configuration	No configuration
Delegation portal configuration	No configuration
Visual model	default
Active	<input checked="" type="checkbox"/>

Add

Create a filtering access for UCOPIA syslog server to the different Cloud Meraki subnets listed above.

[Configuration](#) [Management](#) [Monitoring](#) [Operations](#) [CLI access](#) [Documentation](#) [Restart](#) [Shut down](#)

- **Network**
 - Controller
 - Incoming networks
 - Outgoing networks
 - Static routes
 - Time server
 - DNS server
 - Filtering
- **Authentication**
- **Zero configuration**
- **Customization**
- **Logging**
- **High availability**
- **Out-of-band**
- **External services**

Filtering settings configuration

Adding an access

Note : Access to the controller allows you manage the influx of flows to the service controller

Access settings

Service

Syslog

Sources

Add a source

▶ Subnet

-

Others

/

Active

☒

Add

In « Wireless > Configure > Access control » of the concerned SSID (1/3):

Network-wide

Wireless

Organization

Help

New in Dashboard: A brand new look for switches and 1 other feature. [Read more.](#)

Access control

SSID: OOB Meraki 25-oct ▼

Network access

Association requirements

☒ Open (no encryption)
Any user can associate

☐ Pre-shared key with WPA2 ▼
Users must enter a passphrase to associate

☐ MAC-based access control (no encryption)
RADIUS server is queried at association time

☐ WPA2-Enterprise with Meraki authentication ▼
User credentials are validated with 802.1X at association time

Splash page

☐ None (direct access)
Users can access the network as soon as they associate

☐ Click-through
Users must view and acknowledge your splash page before being allowed on the network

☒ Sign-on with my RADIUS server ▼
Users must enter a username and password before being allowed on the network

☐ Sign-on with SMS Authentication
Users enter a mobile phone number and receive an authorization code via SMS.
After a trial period of 25 texts, you will need to connect with your Twilio account on the [Network-wide settings](#) page.

☐ Billing (paid access)
Users choose from various pay-for-access options, or an optional free tier

☐ Systems Manager Sentry enrollment ⓘ
Only devices with Systems Manager can access this network

In « Wireless > Configure > Access control » of the concerned SSID (2/3):

RADIUS for splash page

#	Host	Port	Secret	Status	Actions
1	cloud1.ucopia.com	1812	*****	OK	+ X Test

[Add a server](#)

RADIUS accounting

RADIUS accounting is enabled [v](#)

RADIUS accounting servers

#	Host	Port	Secret	Status	Actions
1	cloud1.ucopia.com	1813	*****		+ X

[Add a server](#)

Enable data-carrier detect?

DCD is enabled [v](#)

IP addresses

The Meraki cloud must be able to communicate with your RADIUS servers via the Internet.

Please make sure that:

1. Your RADIUS servers have public IP addresses (i.e., they are reachable on the Internet).
2. Your firewall, if any, allows incoming traffic to your RADIUS servers.
3. You whitelist IP addresses as clients on your RADIUS server as per the [firewall information page](#).

Failover policy

If none of your RADIUS servers are reachable, should clients be allowed to use the network?

☒ Deny access

☐ Allow access

Load balancing policy

☒ Strict priority order

☐ Round robin

Network access control

Disabled: do not check clients for antivirus software [v](#)

Assign group policies by device type

Disabled: do not assign group policies automatically [v](#)

Captive portal strength

Block all access until sign-on is complete [v](#)

Walled garden

Walled garden is enabled [v](#)

Walled garden ranges

cloud1.ucopia.com [v](#)

[What do I enter here?](#)

Simultaneous logins

Allow simultaneous devices per user [v](#)

In « Wireless > Configure > Access control » of the concerned SSID (3/3):

IP addresses	<p>The Meraki cloud must be able to communicate with your RADIUS servers via the Internet.</p> <p>Please make sure that:</p> <ol style="list-style-type: none">1. Your RADIUS servers have public IP addresses (i.e., they are reachable on the Internet).2. Your firewall, if any, allows incoming traffic to your RADIUS servers.3. You whitelist IP addresses as clients on your RADIUS server as per the firewall information page.
Failover policy	<p>If none of your RADIUS servers are reachable, should clients be allowed to use the network?</p> <p><input checked="" type="radio"/> Deny access</p> <p><input type="radio"/> Allow access</p>
Load balancing policy	<p><input checked="" type="radio"/> Strict priority order</p> <p><input type="radio"/> Round robin</p>
Network access control	<p>Disabled: do not check clients for antivirus software</p>
Assign group policies by device type	<p>Disabled: do not assign group policies automatically</p>
Captive portal strength	<p>Block all access until sign-on is complete</p>
Walled garden	<p>Walled garden is enabled</p>
Walled garden ranges	<p>cloud1.ucopia.com</p> <p>What do I enter here?</p>
Simultaneous logins	<p>Allow simultaneous devices per user</p>
Controller disconnection behavior	<p>Login attempts on this SSID will be processed by the Meraki Cloud Controller. What should happen to new clients if your Internet uplink is down or the controller is otherwise unreachable?</p> <p><input type="radio"/> Open: devices can use the network without signing in, unless they are explicitly blocked</p> <p><input type="radio"/> Restricted: only currently associated clients and whitelisted devices will be able to use the network</p> <p><input checked="" type="radio"/> Default for your settings: Restricted</p>
<h3>Addressing and traffic</h3>	
Client IP assignment	<p><input checked="" type="radio"/> NAT mode: Use Meraki DHCP</p> <p>Clients receive IP addresses in an isolated 10.0.0.0/8 network. Clients cannot communicate with each other, but they may communicate with devices on the wired LAN if the SSID firewall settings permit.</p> <p><input type="radio"/> Bridge mode: Make clients part of the LAN</p> <p>Meraki devices operate transparently (no NAT or DHCP). Clients receive DHCP leases from the LAN or use static IPs. Use this for shared printers, file sharing, and wireless cameras.</p> <p><input type="radio"/> Layer 3 roaming</p> <p>Clients receive DHCP leases from the LAN or use static IPs as in bridge mode. If they roam between APs their traffic will be forwarded to an AP on the same subnet they originally joined, so they will keep the same IP address.</p>

In « Wireless > Configure > Splash page » of the concerned SSID:

Network-wide

Wireless

Organization

Help

New in Dashboard: A brand new look for switches and 1 other feature. [Read more](#)

Splash page

SSID: OOB Meraki 25-oct

Splash pages on this SSID are enabled because custom RADIUS authentication is enabled. You can change this setting on the [access control subtab](#).

Official themes

☐ Modern NEW

☐ Fluid

Custom themes

☐ Copy of Classic

☐ Copy of Fluid

[Create something new](#)

Custom splash URL

☒ Or provide a URL where users will be redirected:

[What is this?](#)

Customize your page

Message

Splash logo

No logo

[Upload a logo](#)

Splash language: English

Splash behavior

Splash frequency: Every day

[What is this?](#)

Where should users go after the splash page?

☐ The URL they were trying to fetch

☒ A different URL:

Color customization

Color Motif: Plain

	Background	Text	Links
Body			
Content 1			
Content 2			

[Preview](#)

MERAKI CONFIGURATION

In « Network-wide > Configure > General »:

Network time zone

Local time zone

Europe - Paris (UTC +2.0, DST)

Filter by country...

Logging

Syslog servers

Server IP	Port	Roles	Actions
84.14.161.21	514	Flows x URLs x	X

Add a syslog server

SNMP

SNMP access

☒ Disable SNMP on access points in this network

☐ Allow SNMP v1/v2c access using the following community name:

☐ Allow SNMP v3 access using usernames and passphrases

There are no SNMP users for this network

Add an SNMP user